Initiators and all barriers: a dynamic method for all PSAs

- A practitioners view on the practical implication on our PSAs

Presented at the CRA's 8th annual Risk Forum, 4th-5th October 2017
Presenter: Anders Olsson (LR)
Co-author: Marc Bouissou (EDF)

Lloyd's Register

EDF

Working together
for a safer world

Outline

1) **Current "PSA praxis" in terms of mission time and repair**
   - Looking at current guides
   - Current praxis
   - An example with results using current praxis
   - Some reflections
2) **Introduction to Initiators & All Barriers (I&AB) methodology**
3) **Using the I&AB methodology in an Spent Fuel Pool example**
   - Presentation of the PSA model
   - Results using different assumptions about repair times
4) **Conclusions**

Lloyd's Register

EDF

1) Current "PSA praxis" in terms of mission time and repair
Looking at current guides

IAEA-SSG 3 about mission time (refer to §5.49, §5.135 and §9.5)

- Determination of mission times should take into account the time it takes to reach a safe, stable shutdown state that allows long term recovery actions to be taken
  - In many cases this has been taken to be 24 or 48 hours for most initiating events
- Mission times can be very long for some initiating events such as LOCAs
- Termination of the analysis at a fixed mission time may prevent meaningful results from being obtained

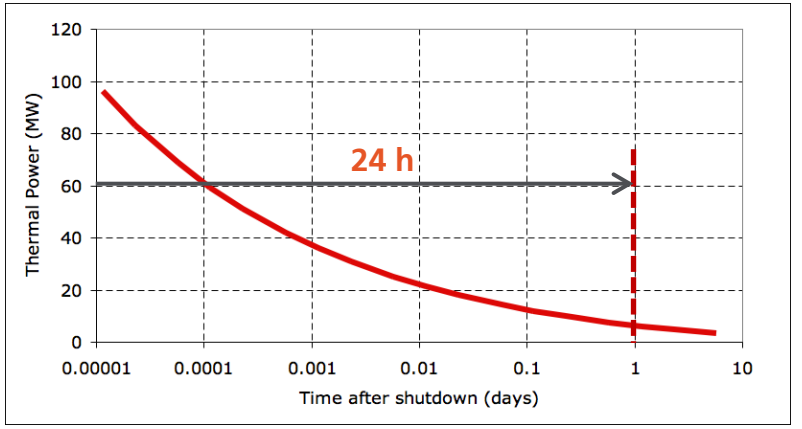
IAEA-SSG 3 about repair (refer to §9.50)

- Repair should be considered since it can increase system availability
- Neglecting repair may lead to an overestimation of risk

1) Current "PSA praxis" in terms of mission time and repair
Current praxis

Statement about current praxis:

- 24 hour mission time for Level 1 (48 h for Level 2) after which there are two possibilities:
  - The plant is in a core/fuel damage state
  - The plant is in a "safe" state which can be managed by plant personnel
    - Numerous options exist and the uncertainties are so large that it is not meaningful to continue the analysis beyond 24 h
- No credit for repair
- All safety systems work in parallel after the initiating event, independently
- A second initiating event cannot occur while the first one is "ongoing"



At the same time the PSA models are being extended to handle more operating modes (e.g. outage),more complex initiating events (e.g. external hazards) and also non-reactor events (e.g. spent fuel pool). PSA is also used as a tool for other facilities with nuclear inventory (e.g. intermediate and final fuel repositories)

1) Current "PSA praxis" in terms of mission time and repair

Current praxis

Statement about current praxis:

- 24 hour mission time for Level 1 (48 h for Level 2) after which there are two possibilities
  - The plant is in a core/fuel damage state
  - The plant is in a "safe" state which can be managed by plant personell
    - Numerous options exist and the uncertainties are so large that it is not meaningful to continue the analysis
- No credit for repair
- All safety systems work in parallel after the initiating event independently
- A second initiating event cannot occur while the first one is "ongoing"

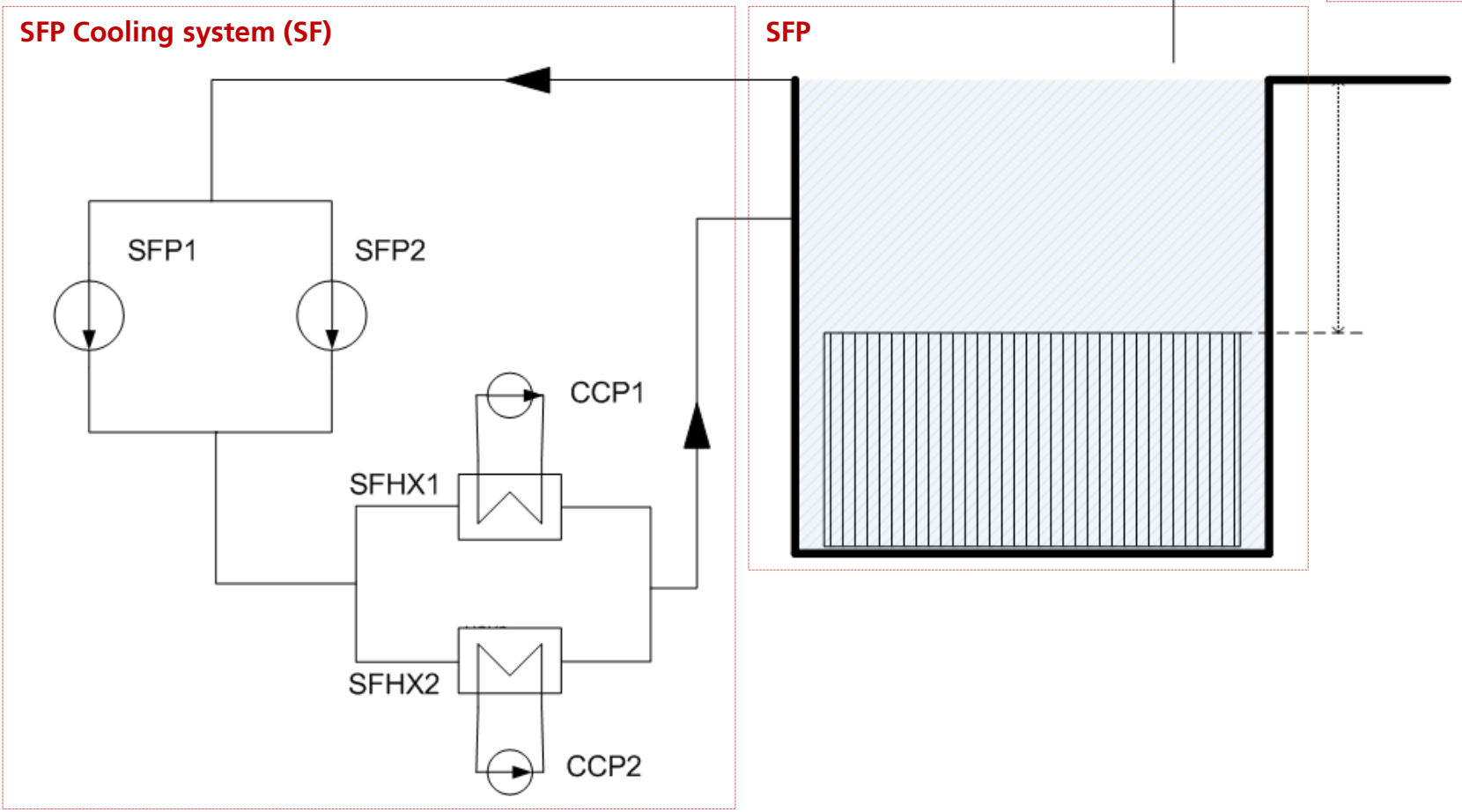
Let's have a look at an example

At the same time the PSA models are being extended to handle more operating modes (e.g. outage),more complex initiating events (e.g. external hazards) and also nor-reactor events (e.g. spent fuel pool). PSA is also used as a tool for other facilities with nuclear inventory (e.g. intermediate and final fuel repositories)

Spent fuel pool cooling

System configuration:
All components in SF and CC systems are in operation.

Stand-by
RW system in stand-by



Spent fuel pool cooling

System configuration:
All components in SF and CC systems are in operation.

Stand-by
RW system in stand-by

Reactor Water Storage (RW)

Fail to start (manual) / Spurious stop

RWP1

RWT1

SFP Cooling system (SF)

SFP

SFP1

SFP2

CCP1

SFHX1

SFHX2

CCP2

Spurious stop (IE) / Fail to run during mission time

Fail to operate, e.g. clogging

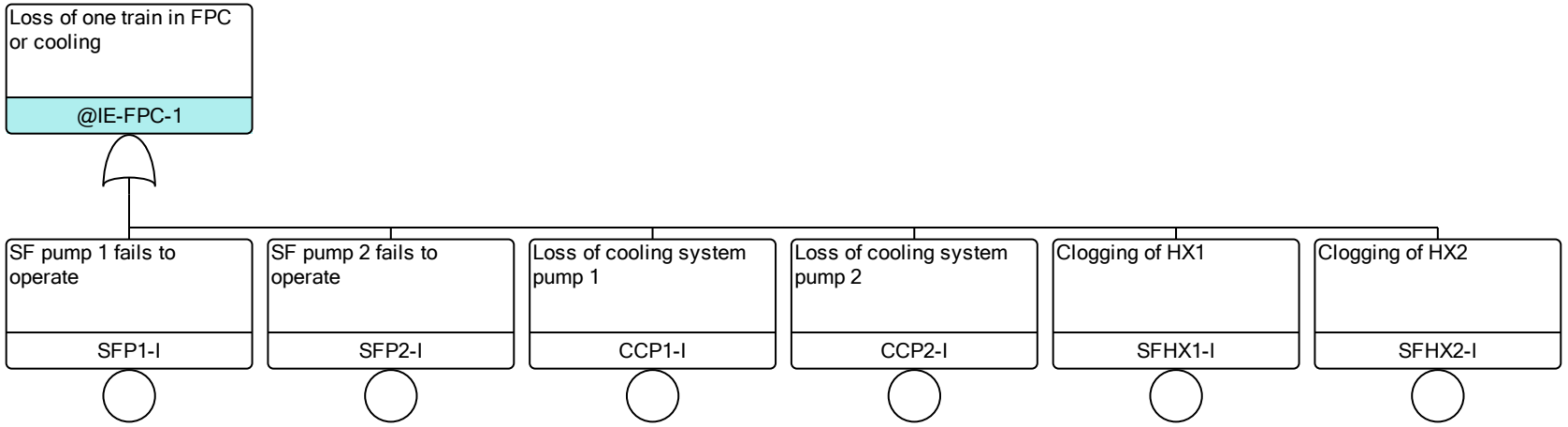
Manual action is necessary in order to activate RW system (assumed covering also start failures)

Mission time in traditional PSA:
- **24 hours for PSA Level 1**
- **48 hours for PSA Level 2**

1) Current “PSA praxis” in the Spent Fuel Pool example

Presentation of the PSA model

Initiator in pool cooling system	Fuel pool cooling system fails	No feedwater to pool				
IE	SFPC	FEED	No.	Freq.	Conseq.	Code
			1			
			2			SFPC
			3			SFPC-FEED



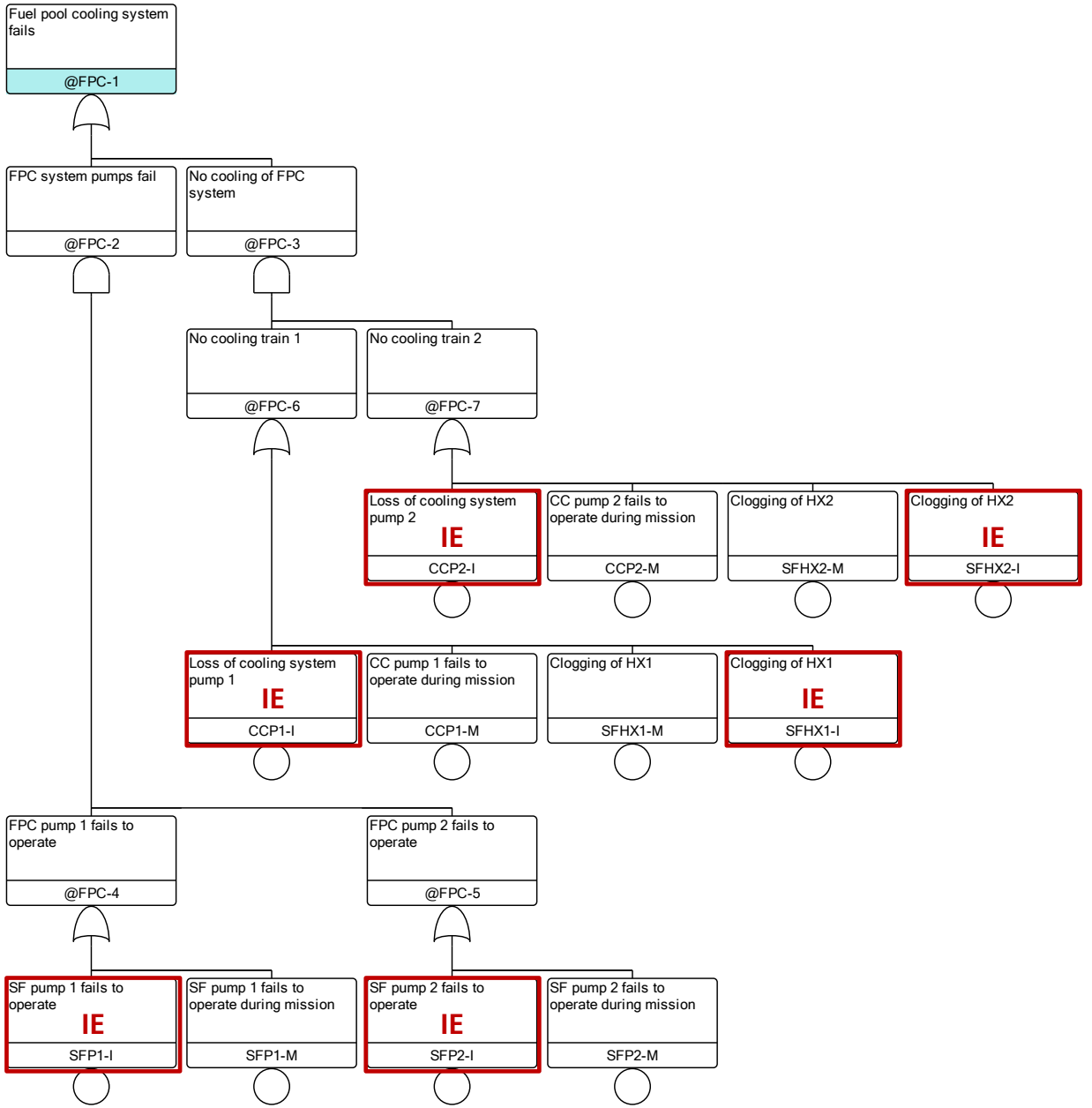
Failure data

- SF pumps: λ = 1E-4/hour
- CC pumps: λ = 5E-5/hour
- HX: λ = 1E-6/hour

1) Current “PSA praxis” in the Spent Fuel Pool example

Presentation of the PSA model

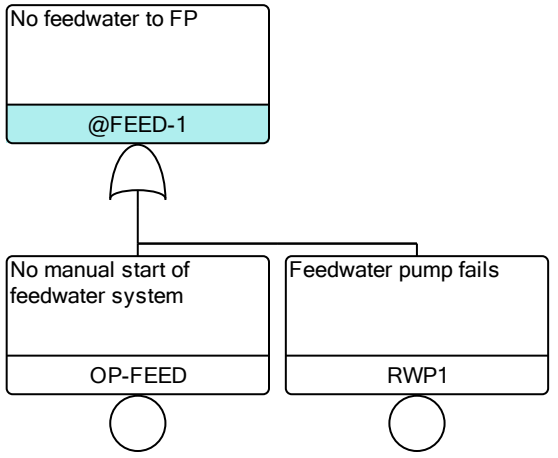
Initiator in pool cooling system	Fuel pool cooling system fails	No feedwater to pool				
IE	SFPC	FEED	No.	Freq.	Conseq.	Code
			1			
			2			SFPC
			3			SFPC-FEED



1) Current “PSA praxis” in the Spent Fuel Pool example

Presentation of the PSA model

Initiator in pool cooling system	Fuel pool cooling system fails	No feedwater to pool				
IE	SFPC	FEED	No.	Freq.	Conseq.	Code
			1			
			2			SFPC
			3			SFPC-FEED



Failure data

- RW pump: λ = 1E-4/hour
- Failure to start: q = 1E-3

1) Current “PSA praxis” in the Spent Fuel Pool example

Some results

- The frequency for ”loss of cooling” is estimated to
  - $1.8 \cdot 10^{-5}$ / year

- Is there a problem with this result?
  - Why 24 hours?
  - Why isn't the repair time of the objects considered?
  - Other parameters that should be taken into account?

1) Reflections on current praxis in PSA regarding mission time

Questions that we should ask ourselves

- **How do we define a safe stable state and how can we demonstrate that it is reached within 24 h?**
  - Many different strategies can be applied >24 h is a common motive
  - What is a safe and stable end state in the SFP example?

- **How do we take into account the duration of the initiating event?**
  - E.g. the duration of "Loss of Off-site Power" can vary
  - What about when IE is repaired, e.g. Off-site Power returns?

- **Is the same mission time as for full power "reactor events" applicable also for e.g. spent fuel pool (SFP) PSA?**
  - In an integrated PSA model covering several operating modes it is not practical to have different mission times for different operating modes

2) Introduction to *Initiators & All Barriers* (I&AB) methodology

Background

- An EDF developed methodology, for further reference see:
  - Presentation at ESREL 2016, proceedings ISBN 978-1-138-02997-2
    - https://www.crcpress.com/Risk-Reliability-and-Safety-Innovating-Theory-and-Practice-Proceedings/Walls-Revie-Bedford/p/book/9781138029972
  - Marc BOUISSOU & Olga HERNU
    - EDF, Industrial Risks Management Department, Clamart, Ile-de-France, France

- A new methodology for calculating the reliability of repairable and reconfigurable systems

- The I&AB methodology is currently being implemented in RiskSpectrum® PSA
- The following slides give an introductory overview of the methodology

2) Introduction to *Initiators & All Barriers* (I&AB) methodology

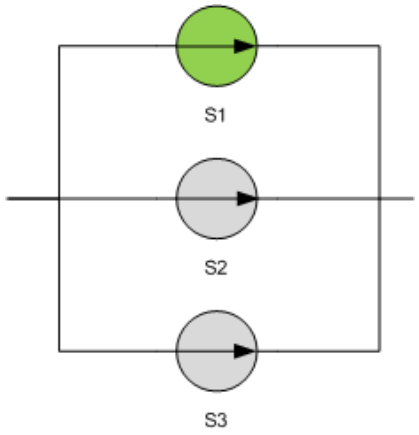
The concept

- I&AB methodology relies on two approximations:
  - When an initiating event occurs, all standby components are supposed to start functioning (or maybe refuse to start) immediately after the initiating event; then, they may fail and be repaired independently from each other until the initiating event is repaired
  - Once an initiating event is repaired, the system cannot fail anymore, whatever happens

- The I&AB methodology uses above approximations and the sequential information that can be found of the Minimal Cut Sets (MCS) identified in the PSA model which can be summarized by the following two features:
  - One, and only one, initiating event in each MCS
  - If the failure of a stand-by component is in a MCS, then component failures for which the stand-by component is a back-up for are also in the MCS

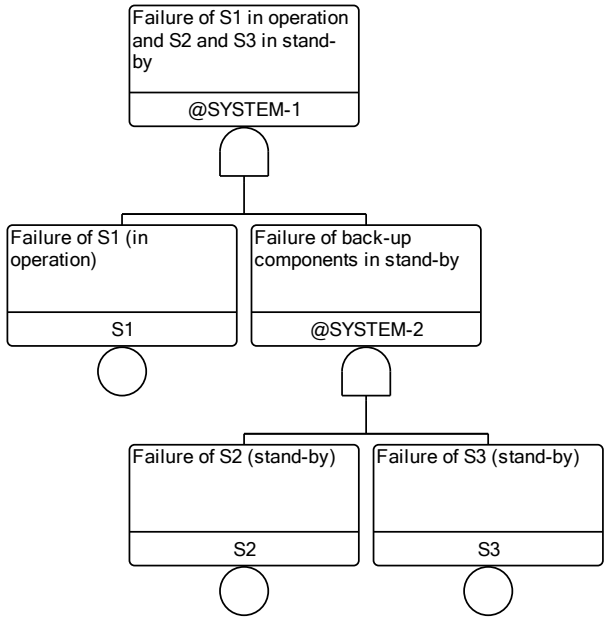
2) Introduction to *Initiators & All Barriers* (I&AB) methodology

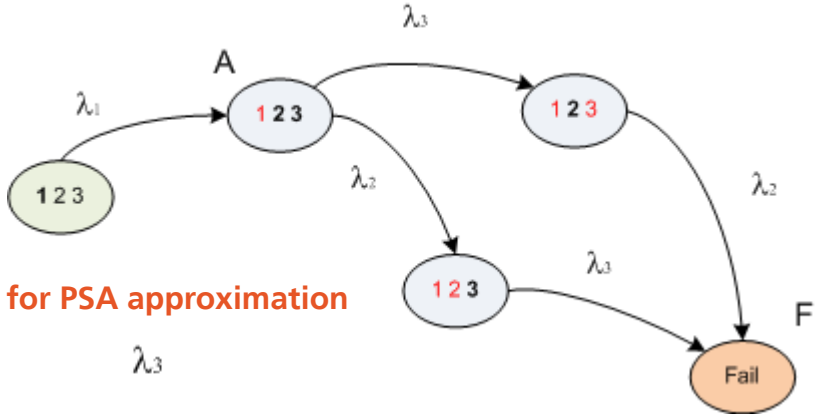
Simplified example of the principle without mathematical formulas



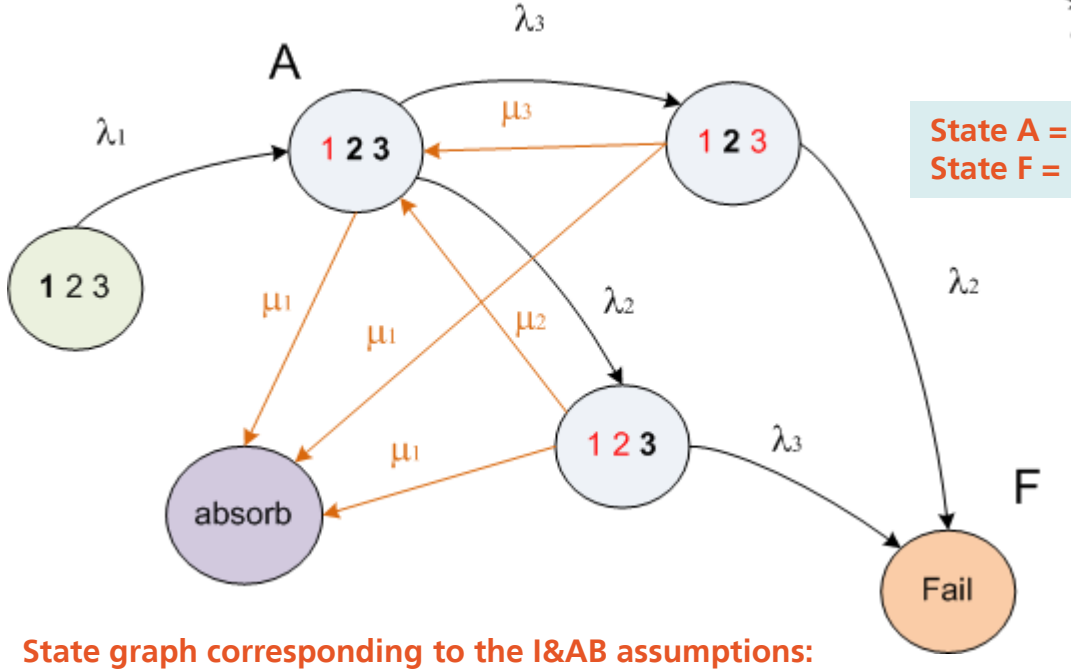
Consider a system of three repairable components where:

- **S1 is in operation; S2 and S3 in stand-by**
- **Failure of S1 require S2 and S3 to start**





State graph for PSA approximation



State A = IE
State F = End state (CD)

State graph corresponding to the I&AB assumptions:

- **Stand-by components start after IE and can be repaired and fail independently**
- **Repair of IE means system cannot fail (absorbed)**
- **No need for mission time**
- **Repair MAY be taken into account**

2) Introduction to Initiators & All Barriers (I&AB) methodology

Some reflections of the characteristics of the method

- The system is required to operate until the initiating event has been "repaired"
  - Different initiators can hence require different "mission time" of the system
- During the required "mission time" repair of the system is considered
  - One component can be repaired when another component is running and then be re-installed again
- Does repair have to be considered for all components?
  - No, repair is considered where it is relevant

3) Using the I&AB methodology in an Spent Fuel Pool example

Consideration of repair

Repair considered for:

- **Initiators:**
  - Spurious stop of pumps,
  - Clogging of heat exchangers
- **Redundant components:**
  - Failure to run for pumps
  - Clogging of heat exchangers
- **Feedwater:**
  - Pump failure to run

Repair not considered for:

- Failure to manually start feedwater system

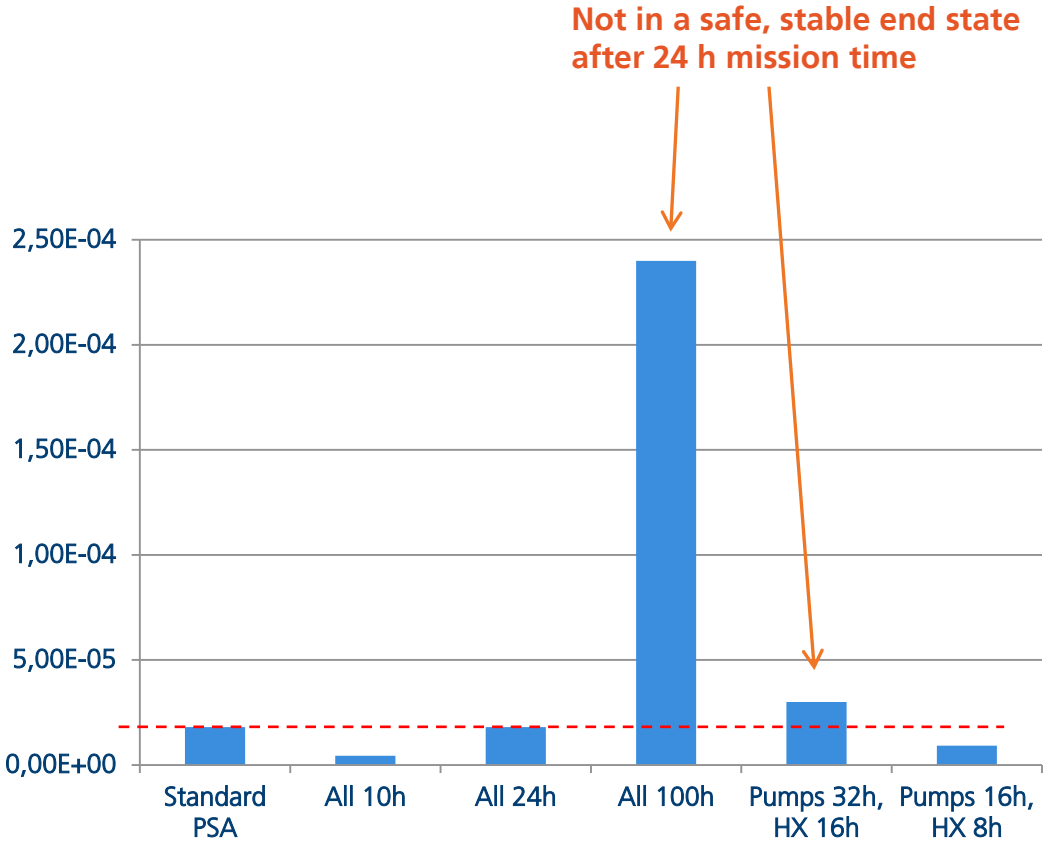
Initiator in pool cooling system	Fuel pool cooling system fails	No feedwater to pool				
IE	SFPC	FEED	No.	Freq.	Conseq.	Code
			1			
			2			SFPC
			3			SFPC-FEED

3) Using the I&AB methodology in an Spent Fuel Pool example

Results using different assumptions about repair times

- Is the 24 hours mission time conservative?

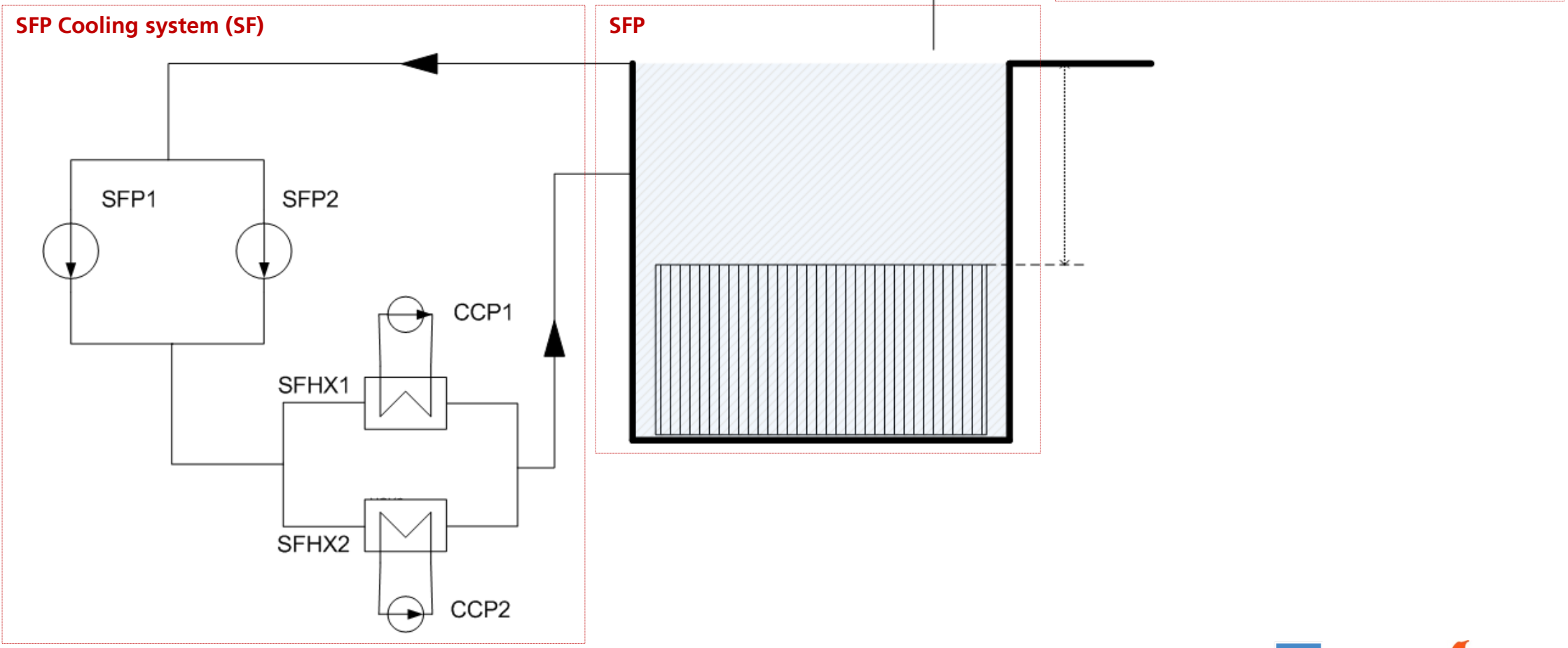
Repair time	Results [1/year]
Reference (standard PSA)	$1.8 \cdot 10^{-5}$
All objects 10h	$4.4 \cdot 10^{-6}$
All objects 24h	$1.8 \cdot 10^{-5}$
All objects 100h	$2.4 \cdot 10^{-4}$
Pumps 32h Heat exchanger 16h	$3.0 \cdot 10^{-5}$
Pumps 16h Heat exchanger 8h	$9.2 \cdot 10^{-6}$



Spent fuel pool cooling

System configuration:
All components in SF and CC systems are in operation.

Stand-by
RW system in stand-by

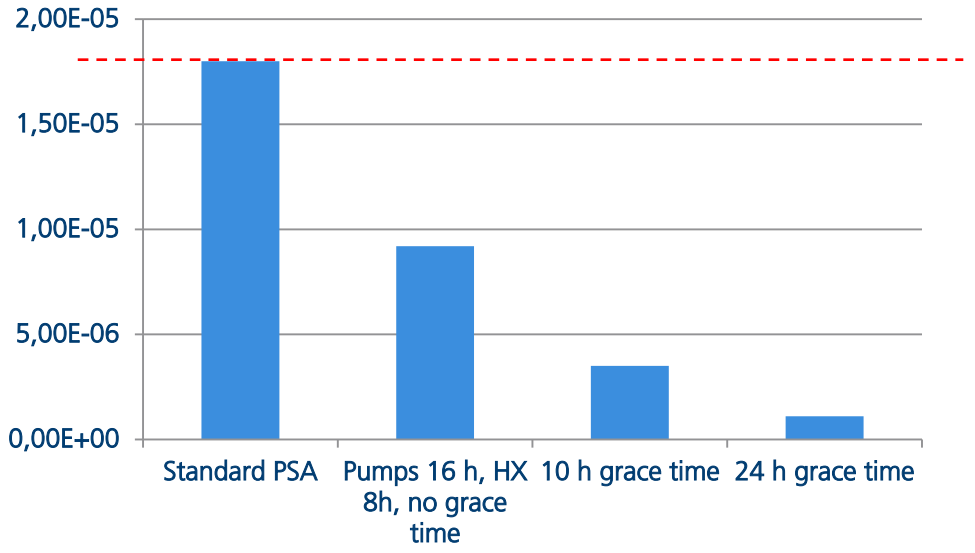


3) Using the I&AB methodology in an Spent Fuel Pool example

Introducing grace times into the calculation

- If the pool cooling system fails, and the feedwater system fails – then that is still not critical
  - Either system can be repaired during the grace time, i.e. before the water in the pool starts to boil
- In this example we have assumed that the grace time is 10 or 24 hours

Repair time	Results [1/year]
Reference (standard PSA)	$1.8 \cdot 10^{-5}$
Repair: Pumps 16h, Heat exchanger 8h	
no grace time	$9.2 \cdot 10^{-6}$
10h grace time	$3.5 \cdot 10^{-6}$
24h grace time	$1.1 \cdot 10^{-6}$

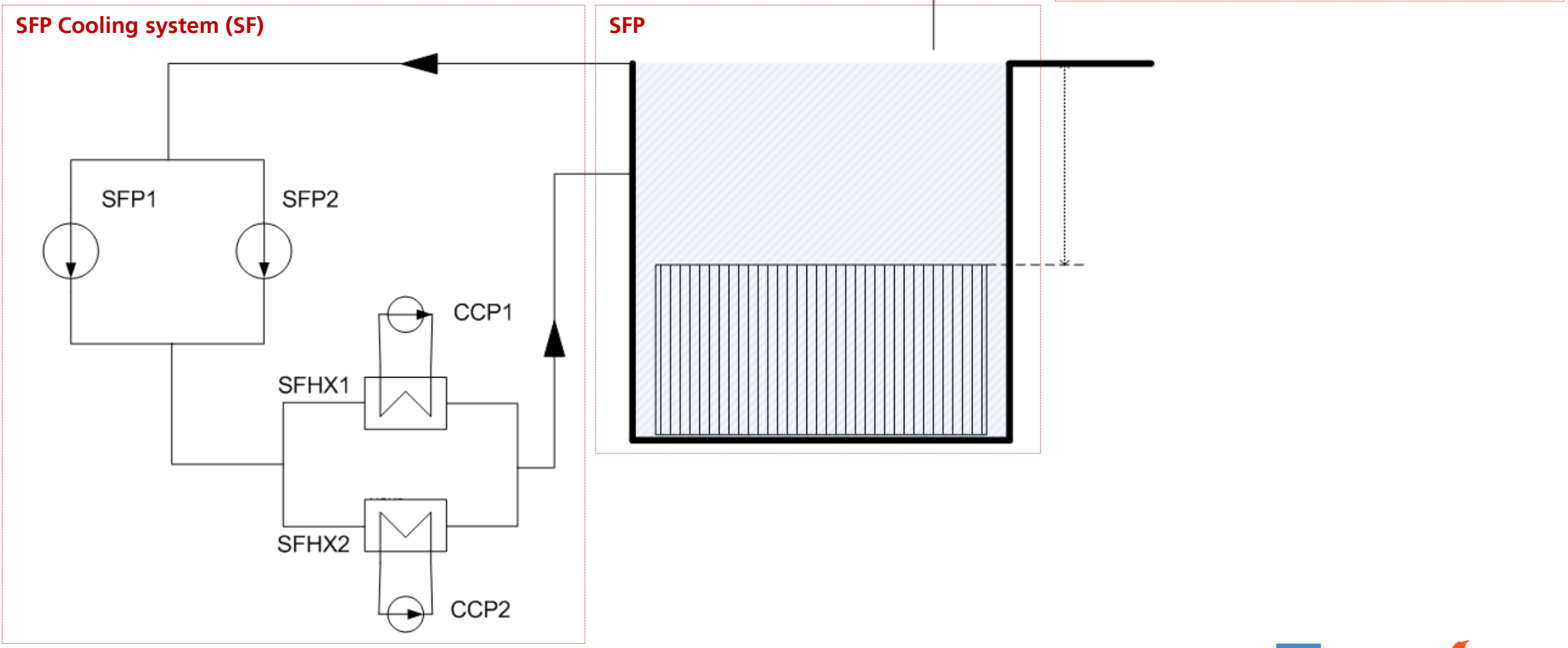


Long grace times increases likelihood for successful repair

Spent fuel pool cooling

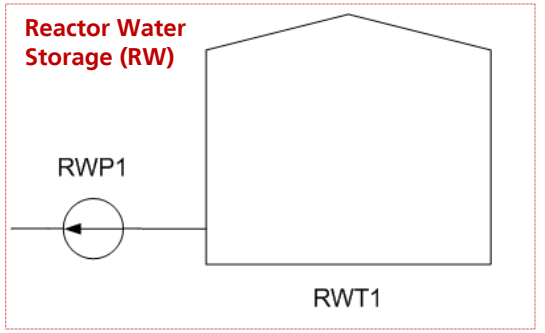
System configuration:
All components in SF and CC systems are in operation.

Stand-by
RW system in stand-by



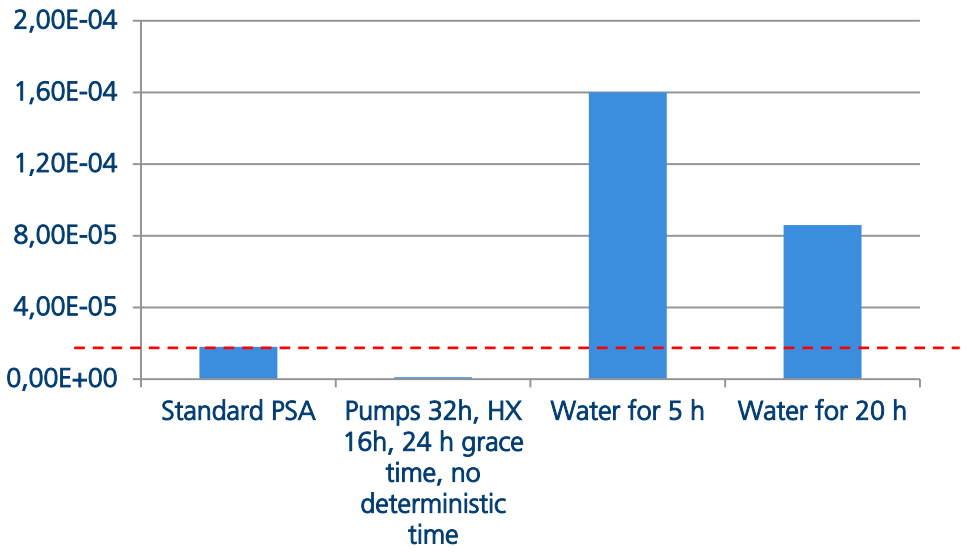
3) Using the I&AB methodology in an Spent Fuel Pool example

Introducing deterministic times into the calculation



- The tank in the example has a finite amount of water
  - How to account for this?
- The system can only be used during the period, during which the tank can provide water
- During this period (or during this period plus the grace time) the other objects can be repaired

Repair time	Results [1/year]
Reference (standard PSA)	$1.8 \cdot 10^{-5}$
Repair: Pumps 16h, Heat exchanger 8h Grace time: 24hours	
No deterministic time	$1.1 \cdot 10^{-6}$
Water for 5 h	$1.6 \cdot 10^{-4}$
Water for 20h	$8.6 \cdot 10^{-5}$



4) Conclusions

What has been demonstrated?

- Use of a fixed mission time of 24 h (current praxis) may be optimistic
- A safe and stable end state should be defined as “when the initiating event is repaired”
- Neglecting repair may be very conservative and can obscure the real risk contributors
- Taking actual grace times into account will improve realism
- Taking deterministic times into account allows for consideration of systems that cannot provide a stable end state
  - Neither optimistic (accounting for it as sufficient) nor pessimistic (not accounting for it)

4) Conclusions

Can – or should – this method also be used in standard PSA?

- It is a completely new methodology that allows for more realistic calculations of safe, stable end states without the necessity of any (arbitrary) mission time being introduced
- The method allows for long term calculations as repair is enabled
- The method can be applied on large scale models

Q&A

I am starting this Q and A thing, so message or comment and ask me a question! Then I will make a video answering the question. :)

Lloyd's Register

EDF

Anders Olsson
Vice President Business Development
T +46 70 733 43 08 E anders.olsson@lr.org

Lloyd's Register
www.lr.org

Lloyd's Register

eDF

Working together
for a safer world